



Universidade de Brasília

Instituto de Relações Internacionais

Programa de Pós-Graduação em Relações Internacionais

XX Curso de Especialização em Relações Internacionais

Guerra Fria 3.0 – o jogo de poder entre Estados Unidos e Rússia no ambiente cibernético

Aline Lopes Ferrer

**Artigo apresentado como requisito parcial para obtenção
do título de Especialista em Relações Internacionais**

Orientadora: Prof. Dr. Thiago Gehre

Brasília

2019

Introdução

Um dos marcos do fim da Guerra Fria entre EUA e URSS foi a queda do muro de Berlim em 1989. O retorno do jogo de poder entre russos e norte-americanos 30 anos depois apresenta contornos de um conflito agora travado no ambiente cibernético, uma Guerra Fria 3.0 que conecta a antiga lógica de disputa de poder com as novas tendências da sociedade da informação e do uso da tecnologia.

Em 8 de novembro de 2016, aconteceram as eleições presidenciais nos Estados Unidos da América. Na disputa bipartidária tradicional, a democrata Hillary Clinton enfrentou o republicano Donald Trump. Durante a campanha, as pesquisas mostravam Hillary na frente, mas a vitória foi de Trump.

A eleição foi cercada de polêmicas. A campanha republicana foi recheada de ataques com notícias falsas sobre Hillary Clinton. Após um ataque de *hackers* aos *e-mails* do partido democrata, levantou-se a suspeita da utilização de criminosos cibernéticos na campanha de Trump.

Eleito presidente, Trump assumiu em 2017 rodeado por essa suspeita e por outras polêmicas envolvendo aliados (como compra de silêncio de prostitutas com dinheiro de campanha). Logo durante o seu primeiro ano de mandato, o FBI iniciou sua investigação e afirmou que *hackers* e *bots* da Rússia espalharam *fake news* e invadiram os *e-mails* do partido.

Trump nega a ligação com os russos e acredita numa “caça às bruxas” contra ele e seus aliados. No entanto, somente a suspeita de interferência foi o suficiente para gerar instabilidade política dentro do país e em sua relação, já historicamente perturbada, com a Rússia.

A ação de *hackers* e *bots* nas eleições norte-americanas de 2016 é um exemplo recente de como a *internet* se tornou um novo espaço onde líderes mundiais podem disputar e demonstrar o seu poder. A informação se torna uma arma de guerra tão poderosa quanto armas nucleares.

O caso norte-americano inunda os telejornais todos os dias desde que as suspeitas começaram a aparecer. É um assunto recente e de grande impacto, por se tratar de dois “inimigos” antigos e da interferência no processo eleitoral da maior potência mundial.

O papel da informação sempre foi tratado como importante, tanto na política externa como interna. A *internet* é um novo espaço de circulação dessas informações de forma mais livre – e perigosa. As faculdades de comunicação ensinam a responsabilidade e os impactos que certas informações podem gerar na sociedade, sendo assim é de tamanha importância que se trate a livre circulação de informação. O estudo dos impactos de informações, principalmente as falsas, é importante para que se possa combater e se possa pensar de forma mais responsável o que se transmite.

Este trabalho tem como objetivo identificar os elementos de instabilidade no âmbito doméstico causados pela suposta interferência cibernética russa nas eleições dos Estados Unidos da América em 2016 e avaliar os impactos causados na relação bilateral entre os países.

1. Estado e Ciberespaço

1.1 Um novo espaço

Para o Departamento de Defesa dos Estados Unidos (U.S. Defense Department, DOD), ciberespaço é “um domínio global dentro do ambiente informacional na rede interdependente de infraestruturas de tecnologia da informação”.

Agentes governamentais, institutos e organizações têm suas próprias concepções do que é ciberespaço. No entanto, há alguns pontos em comum: é um ambiente virtual, composto por redes de infraestrutura que criam espaço de informação. É no ciberespaço que a comunicação flui de forma livre. Segundo Ramonet (2012), o ciberespaço permite que cada cidadão se torne um criador e disseminador de conteúdo, não apenas um consumidor:

[...]nós saímos de um sistema mídia-cêntrico e entramos num sistema eu-cêntrico, em que cada internauta possui o poder de comunicar sons, textos, imagens, de trocar informações, de redistribuí-las, de misturá-las a diversos documentos, de realizar suas próprias fotos ou vídeos e de colocá-los na rede, onde massas de pessoas vão vê-las e, por sua vez, participar, discutir, contribuir, fazer circular. O desenvolvimento das redes sociais renova, assim, o projeto de uma democratização da informação (RAMONET, 2012, p. 28)

Para Bryant (2009, p.48), o conceito de espaço é composto por lugar, distância, tamanho e rota. Segundo o autor, o ciberespaço apresenta esses quatro conceitos, mesmo que não contenha materiais físicos. O ciberespaço é tão espaçoso quanto o espaço real. Há, no entanto, algumas especificidades: a velocidade de ação e reação muda, transformando as relações e o fluxo de informações para uma rapidez nunca antes vista. Por isso, pode apresentar problemas graves para os Estados.

Um Estado é baseado em território, pois é nesse espaço de terra que detém o seu poder. O ciberespaço modifica essa lógica, já que as fronteiras deixam de existir. As fronteiras das informações sigilosas também desaparecem.

1.2 O poder da informação

O fenômeno da comunicação passa a ser levado em conta como fator de importância a partir da década de 1980 com a *Teoria da Ação Comunicativa* de Jürgen Habermas. O autor enfatiza o papel central da linguagem na construção de uma ordem social legítima – onde o diálogo racional constante constrói regras de convivência e valores coletivos e globais (*apud* JATOBÁ, 2013).

Habermas (*apud* JATOBÁ, 2013), então, coloca a racionalidade e o diálogo como centrais. Sendo assim, também diferencia as diferentes formas de racionalidade. A instrumental, que foca no controle da natureza; a estratégica, cujo interesse é na manipulação dos demais atores sociais; e a comunicativa, com preocupação no entendimento e aceitação dos receptores das mensagens.

Nas relações internacionais, Richard Ashley utilizou a *Teoria da Ação Comunicativa* em sua crítica ao realismo político, no livro *Political Realism and Human Interests*. Para o autor (*apud* JATOBÁ, 2013), existem três realismos: o “técnico”, de Kenneth Waltz, cujo interesse é em obter conhecimento para que os Estados aumentem seu poder; o “prático”, de Hans Morgenthau, cujos conhecimentos são baseados em métodos interpretativos; e o “emancipatório”, de John Herz, com a preocupação em assegurar as liberdades.

Andrew Linklater, no entanto, utiliza a teoria de Habermas para fazer uma revisão crítica da teoria marxista, no livro *Beyond Realism and Marxism*. O autor subdivide a terceira forma de

racionalidade em duas: “racionalização diplomática”, com foco na coexistência; e “racionalidade ética”, cuja preocupação é na criação de um código moral.

A Teoria Crítica propõe-se a investigar as causas das desigualdades e injustiças (JATOBÁ, 2013). A teoria de Linklater enxerga o Estado como uma construção social, sendo necessário analisar a racionalização das fronteiras e as exclusões e inclusões sociais. Para ele, é precisa a análise dos “múltiplos eixos de exclusão”. A saída, então, seria substituir a “ética da exclusão” pela “ética do diálogo”, onde cada membro de uma determinada comunidade tem o direito de falar e de ser ouvido.

Entre a década de 1980 e a virada do milênio, a centralidade da informação se mostrou mais forte, sendo utilizada cada vez mais como arma de guerra. Entramos na era “*Post-Truth*”, a pós-verdade.

Em 2016, o Dicionário de Oxford elegeu a palavra pós-verdade como palavra do ano. Higgins (2016) explica que a mentira se torna rotina na sociedade na era da pós-verdade – e a divulgação e compartilhamento de uma mentira não é plausível de condenação. O autor também explica que um relativismo extremo do que é verdade pode tirar o espaço para um debate, mas sustenta que deve-se perceber, pelo menos minimamente, que não há verdade absoluta.

Flores (2017) apresenta um elemento que pode ser considerado o catalisador dessa nova era:

Em um contexto comunicativo cujo conteúdo proposicional possa ser considerado válido, diz-se que o indivíduo comunicador enuncia. Já em um contexto comunicativo cujo conteúdo proposicional apenas pretenda ser considerado válido, diz-se que o indivíduo comunicador insinua. A insinuação se ancora fundamentalmente no princípio de desencadear inferências de natureza falseadora, pelo apelo consciente a crenças ou a impressões arraigadas ao interlocutor (FLORES, 2017, p.22).

O autor argumenta, então, que os fatos passam a ter importância secundária, cedendo espaço para interpretações parciais.

A intenção do indivíduo que insinua é fazer o seu interlocutor diminuir a percepção a respeito daquilo que se veicula no conteúdo proposicional e fazer com que ele amplie a percepção daquilo que parece estar oculto na ação relatada. Desse modo, ao se amparar na transmissão de um conteúdo aparentemente simples, o insinuador se exime da responsabilidade pelas inferências realizadas

pelo interlocutor, seguindo a ideia de que quem fala é responsável por aquilo que diz, não por aquilo que o interlocutor pensa ter entendido (FLORES, 2017, p.26).

Sendo assim, o principal objetivo da pós-verdade é desorientar o leitor no processo de formulação de conhecimento e de opiniões.

1.3 Fake News

Dentro do debate de pós-verdade na era da internet, é preciso compreender que essas produções colocam em cheque noções básicas de autoria, legitimidade e formulação. Para o internacionalista, as informações falsas atrapalham seu trabalho e sua análise, já que é um tomador importante de decisão. Para o jornalista, esse debate se reflete em outro desafio: a perda de espaço e credibilidade de seu trabalho.

Uma pesquisa realizada pelo *Digital News Report 2016* (NEWMAN; FLETCHER; LEVY; NIELSE, 2016), mostra que apenas 56% da população confia nos veículos jornalísticos – e essa confiança cai para 54% quando se refere aos profissionais. Isso mostra que o jornalismo enfrenta um grave problema de confiabilidade.

Segundo Kovach e Rosenstiel (2003), a notícia é o principal produto do jornalismo e é ancorada no instinto de percepção do ser humano. Ou seja, as pessoas necessitam saber os acontecimentos. Os autores também reforçam a importância do ramo e o seu compromisso com a verdade, pois há um consenso entre os profissionais que os fatos devem ser bem apurados e o mais exato possível.

Rumores e boatos existem desde o começo da sociedade humana. São fenômenos que fazem parte da sociedade como um todo, no entanto, o alcance da *internet* e as suas especificidades como plataforma de divulgação de informação fazem com que esses rumores tomem dimensões incalculáveis em formato de notícia: são as *fake news*.

Allcott e Gentzkow (2017) definem *fake news* como “notícias que são intencionalmente e comprovadamente falsas, podendo enganar os leitores”. Ou seja, há a intenção da distorção das informações. Curiosamente, o termo foi fixado pelo então presidente dos Estados Unidos, Donald Trump – apesar de ser uma associação de quebra de credibilidade de veículos notórios, como a CNN.

Um levantamento feito pelo *Buzzfeed* (SILVERMAN, 2016) mostra que mais de 20 histórias falsas foram divulgadas por sites nos três últimos meses de campanha presidencial norte-americana, gerando mais de 8 milhões de compartilhamentos, reações e comentários no *Facebook*. Entre as notícias repercutidas está “Papa Francisco choca o mundo e apoia Donald Trump”, além da falsa associação de Hillary Clinton com o Estado Islâmico e do partido Democrata com tráfico sexual de crianças.

Essas *fake news* impactam a sociedade e preocupam grande parte da mídia. Uma pesquisa realizada pelo *Pew Research Center* (BARTHEL; MITCHELL; HOLCOMB, 2016) mostra que 64% dos americanos entrevistados confundem o que é *fake* e o que é fato. Para combater esse fenômeno, plataformas como o *Google* tentam impedir páginas falsas de anunciarem no seu espaço e jornalistas no mundo se unem para criar agências e *sites* de *fact-checking*.

Para Martin Libicki (2007), o processo de distorção de informações é parte essencial na guerra travada no ciberespaço:

As pessoas impõe as armas nucleares aos outros, mas, como notado, não há penetração forçada no ciberespaço. Os *hackers* têm pouca extensão hábil para criar caminhos de entrada - apenas para explorá-los. Guerra informacional, como notado, é altamente relacionada à enganação de um nível ou outro [...] (LIBICKI, 2007, p. 39).

Segundo o autor, na era da tecnologia da informação, a principal característica é a capacidade de enganar e iludir, em um contexto de guerra não convencional. O ciberespaço se torna, então, um novo campo de disputa de poder.

1.4 Cyberwar

Para Nye (2010), “o ciberespaço não substituirá o espaço geográfico e não destruirá a soberania estatal, mas a difusão de poder no ciberespaço irá coexistir e complicar grandiosamente o que significa o exercício do poder nestas dimensões”. O autor também conceitua o que é poder nesse novo espaço:

Em uma abrangente definição, poder cibernético é ‘a habilidade de usar o ciberespaço para criar vantagens e eventos de influência em outros ambientes operacionais e através de instrumentos de poder.’ Ciberespaço pode ser usada para produzir resultados preferidos dentro do ciberespaço ou pode usar

instrumentos cibernéticos para produzir resultados preferidos em outros domínios fora do ciberespaço (NYE, 2010)

Fora do cibernético, poder significa a capacidade de ter seus objetivos atendidos, para Nye (2010). Já no mundo cibernético, o ciberespaço em si é usado como meio de viabilizador de vantagens de determinados atores que podem ter resultados fora dele.

Nye (2010) também conceitua três faces do poder cibernético. A primeira é a indução de ação, com o recrutamento de *hackers*. A segunda face é o controle de agenda, limitando campo de atuação política dentro do ciberespaço. Já a terceira, é a manipulação e distribuição massificada de informações.

Todas as formas de poder, como o militar, por exemplo, precisam de um exército bem treinado - o poder cibernético não é diferente. Sendo assim, o Estado permanece como o ator principal, já que ele precisa treinar seus *hackers* para atacar ou defender. No entanto, como aponta Nye (2010), um Estado extremamente inserido no ciberespaço também é um grande alvo.

Assim como gera um novo espaço de disputa de poder, o ciberespaço também cria novas vulnerabilidades aos atores. Para Ryan Maness (2015), dois fatores devem ser levados em conta: capacidade de ciber defesa e sua ciber dependência. Para o autor, as capacidades cibernéticas ofensivas se baseiam nos avanços tecnológicos incorporados pelo próprio Estado, já a ciber defesa é a capacidade das autoridades estatais de controlar as informações que entram e saem da *internet*. Maness (2015) apresenta os seguintes exemplos:

State	Cyber-Offense	Cyber-Dependence	Cyber-Defense	Total Score
Iran	4	5	3	12
Great Britain	7	2	4	13
Germany	7	2	4	13
South Korea	6	4	4	14
North Korea	3	9	2	14
United States	9	2	4	15
Israel	8	3	4	15
China	6	4	6	16
Russia	7	3	7	17

Fonte: MANESS, Ryan. Políticas cibernéticas como fonte de poder. 2015. P. 9

Como podemos ver, os Estados Unidos têm uma alta capacidade cibernética ofensiva, resultado da existência de grupos de agentes de inteligência focados nesse novo espaço, baixa

dependência e capacidade de defesa. A Rússia, onde o governo exerce um grande controle sobre o fluxo de informações, tem um maior poder defensivo – nas palavras de Maness, é o ator “mais perigoso” nas relações cibernéticas internacionais.

2. Rússia e Estados Unidos – rivalidade histórica

2.1 Guerra Fria

A chamada Guerra Fria começou ao fim da Segunda Guerra Mundial (1939 - 1945) e se estendeu até a queda da União Soviética, em 1991. Do ponto de vista norte-americano, a disputa se deu por ideologias radicalmente opostas. Na visão ocidental, o lado norte-americano representava a democracia, a liberdade e o acesso às oportunidades. Já o lado soviético, autocracia e limitação de oportunidades – com instituições que favorecem o Partido Comunista (ALCAIPANI; BERTERO, 2012). Estados Unidos e União Soviética criaram, então, um condomínio de poder para ordenar as RI (SARAIVA, 2017).

Durante a Segunda Guerra Mundial, Estados Unidos e URSS lutavam lado a lado em uma aliança fraca, cujo único objetivo era a luta contra Adolf Hitler. George Frost Kennan, criador do conceito da Guerra Fria e conselheiro da embaixada norte-americana em Moscou, alertou o presidente Harry S. Truman do avanço internacional da URSS após a guerra. De acordo com o diplomata, o socialismo e o capitalismo eram antagônicos e Moscou jamais admitiria a existência do capitalismo (SARAIVA, 2017).

Nas palavras do presidente norte-americano Truman, em seu discurso de posse em 20 de janeiro de 1949:

“[...]pessoas de todos os lados estão percebendo que o que está envolvido é o bem-estar material, dignidade humana, e o direito de acreditar e louvar Deus. [...] A filosofia comunista é uma ameaça aos esforços das nações livres sobre recuperação mundial e paz duradoura.” (*apud* ALCAIPANI; BERTERO, 2012)

O mundo, então, era dividido em dois blocos, pois ambos os países procuraram abarcar o máximo de aliados dentro de seu poder. A guerra era travada no campo político, ideológico e até econômico – apesar da URSS nunca ter se tornado uma grande potência econômica. Sendo assim, de acordo com o autor, o triunfo do capitalismo era previsível, já que a União Soviética não tinha o interesse de se desenvolver economicamente (ALCADIPIANI; BERTERO, 2012).

No entanto, de acordo com Saraiva (2017), os soviéticos também não tinham o objetivo de expandir seus ideais para o ocidente. Joseph Stalin tinha total percepção da superioridade atômica norte-americana e de revés em que vivia a União Soviética no âmbito da industrialização e da produção agrícola. Ainda de acordo com o autor, a movimentação soviética de reconstrução do país era com base nas políticas de zona de ocupação. Isso confundiu os diplomatas dos Estados Unidos com um possível projeto expansionista que poderia desafiar seu poder.

O presidente Truman, em 1949, enunciou quatro pontos que deveriam nortear a política externa norte-americana para conter o comunismo: apoio às Nações Unidas e seus diversos órgãos, para fortalecer a democracia no mundo; continuação dos programas de reconstrução econômica à países arrasados pelas duas guerras mundiais (Plano Marshall, 1947); fortalecimento das nações amantes da paz; e um novo programa lançado por seu governo para auxiliar no crescimento econômico das áreas subdesenvolvidas (ALCADIPANI; BERTERO, 2012).

O Ponto IV de Truman tinha como norte levar prosperidade e desenvolvimento às regiões do mundo que seguiam os preceitos defendidos pelos Estados Unidos, afastando, assim, a ameaça comunista desses lugares. Este ponto se tornou programa oficial do governo e, com ele, foi propagado o sistema cultural e social norte-americanos (ALCADIPANI; BERTERO, 2012). Suas palavras viraram doutrina – e um desafio direto à União Soviética (SARAIVA, 2017).

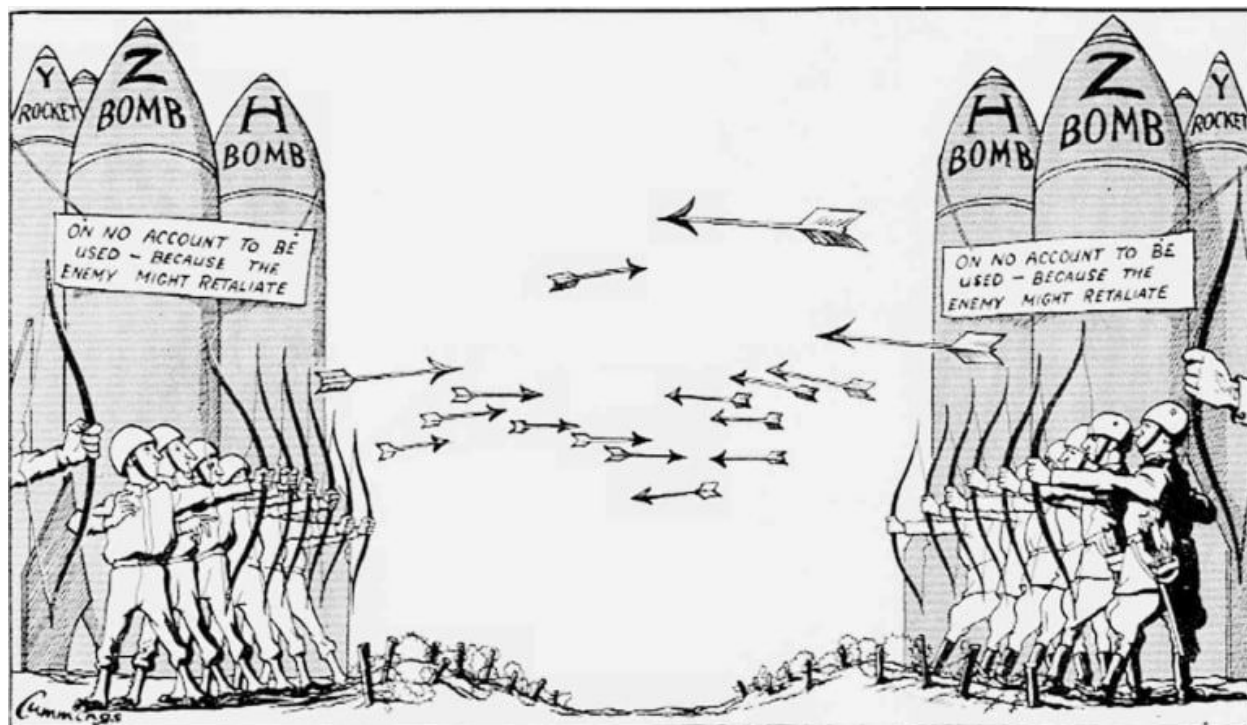
Em abril de 1949, surge a OTAN, a Organização do Tratado do Atlântico Norte. Esta, sendo a “expressão estratégica da febre anticomunista” nos Estados Unidos (SARAIVA, 2017). Doze nações ocidentais se juntaram para um pacto de defesa contra supostas investidas do governo soviético. A OTAN “perpetuava, intensificava e legalizava a presença militar americana no continente europeu” (VIZENTINI, 1990 ,p.26). Criando, assim, um escudo atômico sobre a Europa Ocidental.

As reações soviéticas foram mais lentas. Stalin via a presença norte-americana no leste europeu como ameaça. Em resposta, o Kremlin reiniciou o processo de militarização das fronteiras e acelerou o projeto de criação da bomba atômica. De acordo com Saraiva (2017), a União Soviética conseguiu dobrar o número do efetivo militar de 1947 a 1950. A segunda reação dos soviéticos foi a ampliação do seu espaço para a Europa Oriental, em busca de um equilíbrio

de poder. E foi em 1949 que Stalin fez seu primeiro teste com a bomba atômica. Este equilíbrio atômico se tornou o que Saraiva (2017) chama de “um dos eixos ‘quentes’ da guerra fria até a segunda metade dos anos 1950”.

Em resposta à criação da OTAN, foi realizado o Pacto de Varsóvia, uma aliança militar liderada pela União Soviética. O objetivo, no entanto, era garantir a “manutenção forçada dos países da Europa Central e Oriental no campo socialista do que impedir um ataque ocidental à União Soviética” (ALMEIDA, 2002).

Na segunda metade da década de 1950, no entanto, a guerra esfriou. A chamada “coexistência pacífica” (SARAIVA, 2017) estendeu-se até o final da década de 1960. Este período é marcado pela dificuldade de ambas superpotências de exercerem seu poder. O Plano Marshall deu certo e a Europa voltou ao centro das relações internacionais. Os dois lados se chegaram ao ponto de equilíbrio com suas armas nucleares, causando um “equilíbrio do terror”. Durante esse período, a União Soviética começa a sua desintegração com a ruptura chinesa, tirando o protagonismo único de Moscou no mundo comunista.



Fonte: Swamp Media¹

¹ Disponível em: <<https://theswamp.media/best-vintage-cold-war-political-cartoons>>

Outro fator importante marcou o período da “coexistência pacífica”: a descolonização dos povos da África e da Ásia. A multiplicação repentina de países modificou a dinâmica das Nações Unidas. Ainda fora do eixo EUA – URSS, a América Latina começou a construir seus próprios interesses internacionais, com o objetivo de sair da ideia de “quintal dos Estados Unidos”. Essa movimentação se deu, principalmente, em países como Argentina e Brasil (SARAIVA, 2017).

Até o fim da década de 1970, é o período chamado de *détente*, quando começa a deterioração ideológica do conflito. Ela é marcada pela flexibilização do relacionamento entre as duas superpotências. A bipolaridade já não era vista no âmbito econômico, graças a emergência japonesa. O equilíbrio do terror atômico e a corrida espacial continua a todo vapor. No entanto, Estados Unidos e Rússia começaram a se apresentar como parceiros, com negociações para a limitação de uso e desenvolvimento das armas nucleares.

No fim da década de 1970, o poder soviético começa a cair rapidamente. Os Estados Unidos adotaram o programa armamentista conhecido como “Guerra nas Estrelas”, forçando os soviéticos a engatarem algo semelhante. Essa corrida tecnológica custou caro ao Kremlim. Em 1985, o regime soviético começa a sofrer uma liberalização, com o comando de Mikhail Gorbachev, e o “abandono progressivo do comunismo nos países da Europa Central e Oriental” (SARAIVA, 2017).

A adoção da *perestroika* pelo governo de Gorbachev foi fator decisivo. Segundo Saraiva (2017):

[...] a *perestroika* nunca foi capaz de eliminar os diversos pontos de estrangulamento existentes no campo econômico, tendo, ao contrário, agravado as disfunções já presentes na economia soviética ao não implementar de maneira consequente – como os comunistas chineses o vinham fazendo – mecanismos reguladores de mercado e relações capitalistas de produção e de apropriação em diversos setores da economia (agricultura, pequena produção manufatureira, comércio).” (p. 268)

De acordo com Roberts (1999), a Guerra Fria foi o que modelou a segunda metade do século XX, com consequências sentidas até hoje. O cenário emergente, no entanto, apenas transformou o conceito de zonas de influência, “mas passou a oferecer um único modelo, dito

liberal-democrático de organização política” (SARAIVA, 2017). Portanto, a ruptura do socialismo é considerada uma das mudanças mais radicais no sistema internacional.

No campo da ciência da informação, foi uma época de grandes mudanças e avanços tecnológicos, principalmente nos Estados Unidos. Em 1946, foi construído o ENIAC (*Electronic Numerical Integrator and Computer*), primeiro sistema de computadores. Logo em seguida, em 1947, veio a invenção do micro chip, que consolidou o avanço de pesquisas na área de computação. Os computadores pessoais, como conhecemos hoje, foi desenvolvido a partir da década de 1970, com a invenção do Kenback-1 (1971), Altair 8800 (1975) e o Apple 1, em 1976 (SANTOS JUNIOR, 2012).

2.2 A nova Rússia

Vladimir Putin assumiu o poder russo em 1999, quando o país passava por uma grave crise, após as primeiras tentativas de medidas liberalizantes no país. Putin é um ex-agente da KGB, serviço secreto de segurança da União Soviética e era uma figura relativamente nova na política Russa. Em 30 de dezembro de 1999, um dia antes de assumir o poder, publicou um texto nos jornais onde argumentava a necessidade de adequação ao mundo capitalista, ao mesmo tempo que defendia um papel maior do Estado na regulamentação da sociedade russa. Pelo seu passado como agente, Putin se cercou de oficiais de inteligência (DAWISHA, 2016). O presidente concedeu mais poder à FSB, serviço de segurança federal, que passou a proteger o território de espões e também a desacreditar a mídia televisiva, com a invasão da NTV por agentes que acusaram a empresa de corrupção.

No início de seu governo, Putin parecia sinalizar a manutenção da aproximação com os Estados Unidos após a queda da União Soviética. Após os atentados de 11 de setembro de 2001, a Rússia colaborou com os norte-americanos contra o terrorismo jihadista – apoiaram a intervenção no Afeganistão e permitiram a instalação de bases norte-americanas em países antes soviéticos da Ásia Central. Para os russos, esse apoio era importante, já que estava enfrentando ataques terroristas desde a primeira guerra da Chechênia, em 1994 (MAZAT; SERRANO, 2012).

Em 2002, a Rússia se tornou “parceiro institucional privilegiado da OTAN”, com a perspectiva de “participar da organização da segurança coletiva na Europa” (ECKERT, 2004).

No mesmo ano, integrou o G7, que se tornou G8. No entanto, Putin deixou transparecer rapidamente sua visão de defesa dos interesses nacionais, que teriam sido ignorados nos anos 1990 (MAZAT; SERRANO, 2012).

Na chamada “cruzada contra o eixo do mal”, em 2003, a Rússia se recusou a apoiar a intervenção no Iraque. Em 2007, se opôs o projeto de escudo antimísil, que seria instalado na Europa Central – a ideia era a proteção dos membros da OTAN contra o Irã (BRAUN, 2009). Um ano depois, Putin declara que instalaria estações móveis de mísseis no meio do território polonês.

É nesse contexto que a Rússia passa a utilizar-se da mais nova tecnologia da época: a *internet*. Com a estatização da comunicação midiática e o descrédito da mídia televisiva, as redes sociais passam a ser ferramentas essenciais. Em 2011, após as eleições parlamentares, grandes protestos organizados pelas redes sociais atingiram o país². Emily Parker escreve, em 2014, sobre a “*Cyberphobia*”³ de Putin, argumentando que o governo passou a temer pela estabilidade após a organização de grupos *online*. Dessa forma, começou-se a regulamentação do acesso *online* no país – ao mesmo tempo que perceberam as vantagens que poderiam ser adquiridas nesse novo espaço (REVERON, 2013).

2.3 A presença Russa na *internet*

Após o fim da União Soviética, a Federação Russa passou a implementar medidas de controle e monitoramento das comunicações do país – primeiro dos telefones e depois das comunicações via *internet* (Statewatch, 2000). Essas informações são controladas pelo então FSB, polícia federal sucessora do KGB.

Aos poucos, os sistemas de vigilância foram se aperfeiçoando. O SORM foi criado em 1995 e permite pesquisa e monitoramento das comunicações dos cidadãos. Em 1998, com a explosão da *internet*, foi criado o SORM 2, que aumentou as possibilidades de vigilância para o – então – novo modelo de comunicação (RAMOS, 2012).

² BBC. Russian election: biggest protests since fall of USSR. 2011. Disponível em: <http://www.bbc.com/news/world-europe-16122524>

³ PARKER, Emily. Putin’s Cyberphobia. 2014

No entanto, a *internet* não é só um espaço de vigilância doméstica. A doutrina militar da Federação Russa de 2010, diz:

“[Prioridade das forças armadas] d) a implementação prévia de medidas de guerra de informação para alcançar objetivos políticos sem a utilização da força militar e, subsequentemente, no interesse de moldar uma resposta favorável para a comunidade mundial pela utilização da força militar (RUSSIAN MILITARY DOCTRINE, 2010).

Ou seja, as operações de informação também servem para atingir objetivos políticos. Segundo Nye (2010), o governo russo ignora e protege *hackers* criminosos dentro do ciberespaço e passa a contar com os seus serviços – criando um ciber-exército. A Rússia passou, então, a utilizar recursos não-estatais, *hardwares* e robôs que provocam discussões políticas. São os *trolls*, que atuam para polarizar o debate ou dar a falsa impressão de um apoio maior a determinada agenda⁴.

O grupo acusado pela inteligência norte-americana de ocasionar vazamentos de documentos secretos na NSA que afetaram as eleições de 2016 chama-se *Fancy Bear*. Este grupo não é oficialmente ligado ao governo russo⁵. No entanto, em 2017, Vladimir Putin afirmou que *hackers* patrióticos poderiam ter se envolvido nas eleições norte-americanas⁶. De acordo com o presidente, esses indivíduos não são ligados ao governo, mas se sentiram ofendidos por atores contrários ao país e viram em suas ações uma forma de ajuda à Rússia.

3. Eleições norte-americanas de 2016

3.1 Acusação de interferência

As eleições norte-americanas de 2016 tinha como candidatos Hillary Clinton, a favorita, pelos democratas, e Donald Trump, pelos republicanos. A própria candidatura de Trump foi uma surpresa nas preliminares e atraiu a atenção da mídia pelo seu discurso conservador e radical.

⁴ FOKIN, Alexander. Internet Trolling as a tool of hybrid warfare: The case of Latvia. NATO Strategic Communication Centre of Excellence. 2016.

⁵ Wired. Russia's Fancy Bear hackers. Disponível em: <https://www.wired.com/story/fancy-bear-hotel-hack/>

⁶ The Independent. Vladimir Putin hints at 'patriotic' private hackers interference in US election. 2017. Disponível em: <http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html>

Durante a campanha, Trump utilizou, além dos debates, as mídias sociais para atacar sua adversária. Assim, o *Twitter* se tornou parte importante na vida política norte-americana.

Ainda durante a campanha, milhares de *e-mails* do Comitê Democrático Nacional (DNC), que comanda o partido Democrata, foram vazados. Neles continham informações que ocasionaram uma crise interna.

Esses vazamentos, segundo empresas de segurança cibernética como a *SecureWorks*, *CrowdStrike* e *Threat Connect*, foram realizadas pelos grupos russos *Fancy Bear* e *Cozy Bear*. Os democratas, então, passaram a acusar os russos de interferir nas eleições. O governo russo, no entanto, nega o envolvimento.

Em 31 de outubro de 2017, representantes do *Google*, *Facebook* e *Twitter* prestarem depoimentos perante o Senado norte-americano. Colin Stretch⁷, representante do *Facebook* afirmou:

Agentes estrangeiros, escondidos por trás de contas falsas, abusaram da nossa plataforma e de outros serviços de internet para tentar semear divisão e discórdia, e para tentar minar o nosso processo eleitoral. É um ataque à democracia e viola todos os nossos valores (COLIN STRETCH, 2017)

No momento, há uma investigação em curso no FBI sobre uma possível interferência e a colusão das ações da campanha de Trump com o governo de Vladimir Putin. As redes sociais passaram a banir páginas, propagandas e contas *fakes* de suas plataformas. O *Twitter* anunciou, em 26 de outubro de 2017, o bloqueio de contas relacionadas aos canais russos *Sputnik* e RT⁸.

Por mais que a interferência ainda não tenha sido provada, a investigação mexe com a política interna e aumentou a polarização entre apoiadores de Donald Trump e democratas. Mesmo que Putin e Trump jamais tenham se unido, a própria desconfiança da ação dos *hackers* desestabilizou a cena política do país.

O que se tem de prova é que alguns gigantes da mídia russa divulgaram notícias sobre Hillary Clinton, em inglês, com conteúdos de difamação de sua imagem⁹; e especialistas também

⁷ Testemunho no Senado dos Estados Unidos

⁸ BBC. Twitter bans RT and Sputnik ads amid election interference fears. 2017. Disponível em: <http://www.bbc.com/news/world-us-canada-41766991>

⁹ RT. Role of Hillary Clinton in Lybia war exposed. 2016. Disponível em: <https://www.rt.com/usa/334400-hillary-clinton-libya-role/>

afirmam que *hackers* russos invadiram as contas do DNC¹⁰ - além dos depoimentos dos representantes de grandes companhias de tecnologia.

3.2 Processos

Segundo o então diretor do FBI, James Comey, em testemunho para o Comitê de Inteligência da Câmara, em março de 2017, a polícia já estava conduzindo uma investigação sobre supostas interferências russas desde julho de 2016. Comey afirmou, no entanto, que o FBI nunca chegou a investigar Trump pessoalmente¹¹. A partir daí, o Comitê de Inteligência do Senado e da Câmara criaram suas próprias investigações.

Em maio de 2017, já com Trump presidente, Comey foi demitido. De acordo com ele, a demissão se deve pela insatisfação com a investigação. Outra investigação foi aberta sobre uma suposta tentativa de obstruir a justiça¹². Segundo o jornal *The New York Times*, após a demissão, o FBI se sentiu “instigado” a abrir uma investigação criminal para saber se Trump também trabalha para os russos¹³. Desde então, o procurador especial Robert Muller investiga de forma independente os possíveis laços entre pessoas ligadas a campanha de Trump e a Rússia.

Em fevereiro de 2018, a justiça americana acusou formalmente 13 russos e 3 entidades do país de interferir nas eleições. De acordo com a acusação, eles se passavam por cidadãos americanos através de roubo de identidade de americanos reais. Ainda afirmam que o objetivo era de apoio a Donald Trump, pois chegaram a se comunicar com “indivíduos não conscientes associados à Campanha Trump e com outros ativistas políticos para procurar coordenar atividades políticas”¹⁴.

Ainda segundo o Departamento de Justiça dos Estados Unidos, eles usavam a plataforma *Facebook* para recrutar cidadãos norte-americanos para manifestações, tendo até oferecido

¹⁰ The Guardian. DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach. 2016. Disponível em: <https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2>

¹¹ Fonte:

<https://www.theguardian.com/us-news/2017/mar/20/fbi-director-comey-confirms-investigation-trump-russia>

¹² Fonte: <https://edition.cnn.com/2017/06/14/politics/robert-mueller-donald-trump/index.html>

¹³ Fonte: <https://www.bol.uol.com.br/noticias/2019/01/14/nunca-trabalhei-para-a-russia-diz-trump.htm>

¹⁴ Fonte:

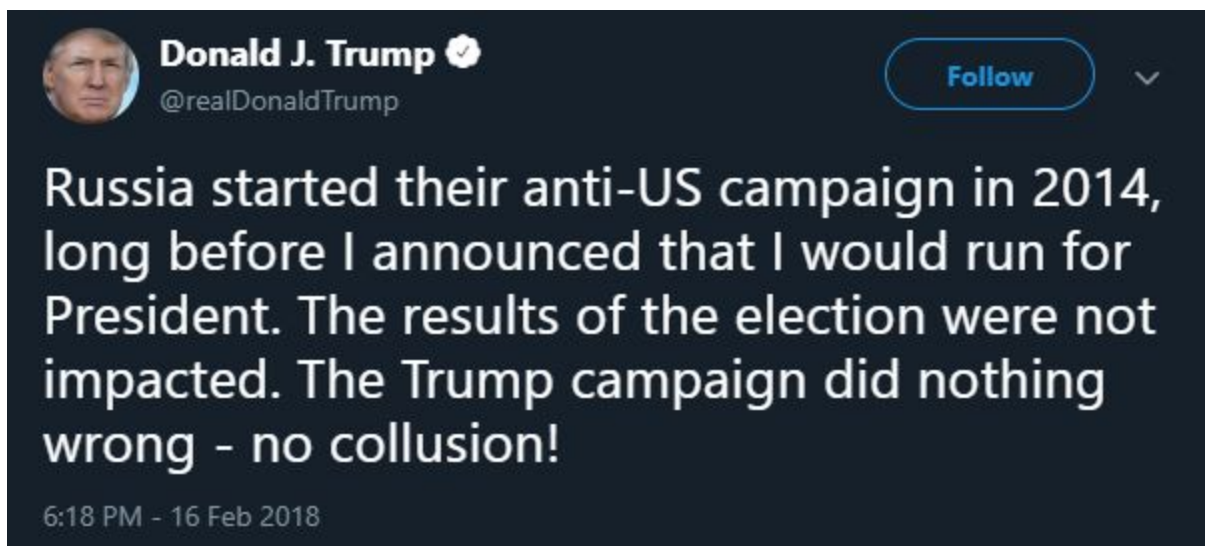
<https://g1.globo.com/mundo/noticia/justica-americana-indicia-13-russos-acusados-de-interferir-na-eleicao-dos-eua.g.html>

dinheiro para a confecção de cartazes e compra de um megafone. Na plataforma, eles compraram anúncios para promover manifestações anti-Hillary Clinton.

Segundo um estudo da Universidade de Oxford, em documento entregue ao Senado norte-americano, as informações falsas foram disseminadas em todas as principais plataformas: *Facebook, Twitter, Tumblr, Pinterest, Instagram, Youtube* e *Google+*. Para os eleitores conservadores, os temas principais eram sobre controle de armas e imigração. Já para o resto do eleitorado, o objetivo era causar dúvida ao processo eleitoral, levando informações falsas sobre como votar¹⁵.

O procurador Rod Rosenstein, no entanto, afirma que não há indícios da participação de norte-americanos e ainda não há provas suficientes para afirmar que essa movimentação russa modificou o resultado da eleição.

Donald Trump utilizou a plataforma *Twitter* para responder as acusações:



Fonte: *Twitter*¹⁶

A porta-voz do Ministério das Relações Exteriores da Rússia, Maria Zakharova, afirmou que as acusações são absurdas. No entanto, entre fevereiro e julho de 2018, 25 cidadãos russos

¹⁵ Fonte:

<https://www.publico.pt/2018/12/17/mundo/noticia/novo-relatorio-revela-maior-dimensao-interferencia-russa-eua-1855030>

¹⁶ Tradução livre: “Rússia começou sua campanha anti-EUA em 2014, muito antes de anunciar que concorreria à presidência. Os resultados da eleição não foram impactados. A Campanha Trump não fez nada de errado – não há coalizão!”

foram indiciados, sendo doze deles acusados de invadir as contas de e-mail da campanha democrata¹⁷. Ao menos onze associados ligados a Trump admitiram contato com os russos durante e depois da campanha presidencial¹⁸. Entre eles, Michael Cohen, advogado pessoal que admitiu ter mentido no Congresso sobre a construção de uma filial da *Trump Tower* (hotel da família Trump) em Moscou¹⁹.

Em janeiro de 2019, o antigo conselheiro de Trump, Roger Stone, foi preso na Flórida acusado de sete crimes relacionados às investigações: cinco acusações por declarações falsas, uma por adulteração de testemunhas e uma por obstrução de justiça. Durante a campanha, Stone teria admitido ter conhecimento sobre informações obtidas por *hackers*. Segundo a acusação, Stone “enviou e recebeu numerosos *e-mails* e mensagens de texto durante a campanha de 2016 nos quais debatia a Organização 1, a sua direção e a posse de *e-mails* pirateados”[19 2]. No entanto, não há acusação sobre articulação direta de Stone com os russos e a Casa Branca continua a negar o envolvimento do presidente Trump.

3.3 Pontos de instabilidade

Em julho de 2018, Donald Trump e Vladimir Putin se encontraram em Helsinque, Finlândia. No encontro, Trump considerou desastrosa a investigação e afirmou que “não houve nenhuma interferência, todo mundo sabe disso. Nós conduzimos uma campanha histórica e é por essa razão que eu sou presidente.”²⁰

Após negar, Donald Trump cedeu uma entrevista à rede CBS de televisão alguns dias depois onde afirmava que a Rússia interferiu nas eleições e apontou Vladimir Putin como responsável. “Vou ser totalmente claro: eu aceito a conclusão da nossa inteligência de que houve

¹⁷ Ver: <https://edition.cnn.com/2018/07/13/politics/russia-investigation-indictments/index.html>

¹⁸ Ver: <https://thehill.com/homenews/administration/392662-roger-stone-russian-wanted-trump-to-pay-2m-for-dirt-on-clinton-during>

¹⁹ Ver: <https://www.usatoday.com/story/news/politics/2018/11/29/michael-cohen-robert-mueller-trump-plea-deal/2147323002/>

²⁰ Ver: <https://noticias.uol.com.br/ultimas-noticias/rfi/2018/07/16/russia-nao-interferiu-nas-eleicoes-americanas-afirma-trump-em-helsinque.htm>

intromissão russa nas eleições de 2016”, afirma. Ainda de acordo com Trump, a Rússia não teria mais os Estados Unidos como alvo²¹.

No entanto, em março, Washington impôs sanções ao Kremlin: 19 cidadãos russos e cinco empresas foram afetados, tendo suas propriedades bloqueadas em território nacional e proibição de operar e fazer negócios no sistema norte-americano. No entanto, o processo não cita como certa, apenas como “tentativas” de interferência nas eleições²².

Em setembro de 2018, foi a vez da Rússia de acusar os Estados Unidos de interferência política. Segundo o *The New York Times*, o Departamento de Justiça e o FBI tentaram obter informações de oligarcas próximos ao presidente russo entre 2014 e 2016, para recrutar cidadãos do país²³.

O vice-ministro russo das Relações Exteriores, Serguei Riabnov, também acusou o país de “inventar” acusações para impor novas sanções, após a prisão de uma cidadã russa acusada de intervir nas eleições²⁴.

No Fórum Econômico Mundial, o secretário de Estado norte-americano, Mike Pompeo, disse que ambos os países não estão “condenados a uma rivalidade da Guerra Fria”²⁵. Vladimir Putin também já tinha se pronunciado e disse não querer uma nova corrida armamentista, abrindo espaço para um “diálogo sério” com os Estados Unidos.

No âmbito doméstico, as eleições legislativas de 2018 colocaram os democratas no centro do governo - tornando Washington um ambiente polarizado. Representantes do partido já afirmaram estarem esperando o relatório de Robert Muller para protocolar um pedido - e prometeram, desde novembro de 2017, investigar cada aspecto da vida do presidente²⁶. No

²¹ Fonte:

<https://www1.folha.uol.com.br/mundo/2018/07/trump-volta-atras-e-diz-que-russia-interferiu-na-eleicao-americana-de-2016.shtml>

²² Fonte: https://brasil.elpais.com/brasil/2018/03/15/internacional/1521127559_111250.html

²³ Fonte: <https://veja.abril.com.br/mundo/russia-acusa-agencias-dos-eua-de-interferencia-politica/>

²⁴ Fonte:

https://www.em.com.br/app/noticia/internacional/2018/10/20/interna_internacional.998766/russia-acusa-eua-de-inventar-acusacoes-de-suposta-interferencia.shtml

²⁵ Fonte: <https://br.sputniknews.com/russia/2019012213161548-russia-eua-guerra-fria/>

²⁶ Fonte:

https://www.washingtonpost.com/lifestyle/style/get-used-to-it-the-i-word--impeachment--is-about-to-dominate-trump-coverage/2019/01/18/0d488fc6-1b44-11e9-8813-cb9dec761e73_story.html?noredirect=on&utm_term=.6053602728f4

entanto, de acordo com o jornal *The Washington Post*, apenas um terço dos cidadãos norte-americanos votantes desejam o *impeachment* de Trump²⁷.

Considerações finais

Os analistas internacionais enfrentam um desafio gigante no século 21: vencer a era da pós-verdade e eliminar as *fake news*. No entanto, esse desafio também é dos representantes de Estado, pois essa desinformação pode causar problemas políticos, tanto no âmbito doméstico quanto no internacional.

No âmbito das *fake news*, Trump não é apenas um alvo, mas um disseminador - o que transforma o problema em algo muito mais complexo para a sociedade norte-americana. Durante sua campanha, ele próprio utilizou informações falsas e teorias da conspiração espalhadas pela *internet* - e o próprio chamou de *fake* as investigações sobre a suposta interferência russa.

Em março de 2019, o procurador especial Robert Muller entregou o seu relatório final para o procurador geral Rod Rosenstein²⁸. Até o fechamento deste artigo, o conteúdo do relatório não foi divulgado publicamente.

Apesar das investigações, a relação pessoal entre Trump e Putin sempre pareceu boa. Trump negou que a interferência teria partido de Putin ou do Kremlim, como um todo. Ao longo do tempo, no entanto, o ciberespaço se tornou apenas uma das áreas instáveis no relacionamento entre os países. Durante as investigações, a tensão aumentou em outros pontos, como a proposta de encerramento do acordo nuclear e a crise política e social na Venezuela.

A suposta interferência nas eleições norte-americanas pode ter sido tratada como “suposta” por dois anos, mas foi motivo para instabilidades tanto domésticas quanto na relação bilateral. Até então, as atividades de *hackers* eram consideradas as mais perigosas no meio cibernético. No entanto, esse caso trouxe à tona que a velha estratégia de espalhar rumores e mentiras para manipular a opinião pública ainda é uma ameaça - e com a *internet*, essa ameaça se torna maior ainda. Como afirmou Julian Assange, fundador do *WikiLeaks*: “[...] não há separação

²⁷ Fonte:

https://www.washingtonpost.com/opinions/2019/01/04/trump-wants-witch-hunt-are-democrats-about-give-it-him/?utm_term=.c9cf321058eb

²⁸ Fonte: <https://edition.cnn.com/2019/03/22/politics/robert-mueller-report/index.html>

entre o que nós pensamos que é uma sociedade, indivíduos, burocracia, Estado e *internet*. A *internet* é o alicerce da sociedade [...]”.

REFERÊNCIAS BIBLIOGRÁFICAS

ALCADIPANI, Rafael; BERTERO, Carlos Osmar. Guerra Fria e o ensino do *management* no Brasil: O caso da FGV-EAESP. In: RAE, v. 52, n. 3. São Paulo: maio/jun. 2012. P. 284-299. Disponível em: <<http://bibliotecadigital.fgv.br/ojs/index.php/rae/article/view/30501>> Acesso em 10 jan. 2019.

ALMEIDA, Paulo Roberto de Almeida. OTAN e o fim da Guerra Fria. In: Revista Espaço Acadêmico, ano 1, n° 9.

ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, 31(2): 211-36, 2017. Disponível em: <<https://goo.gl/TLYvEP>> Acesso em: 16 ago. 2018.

BARTHEL, Michael; MITCHELL, Amy; HOLCOMB, Jesse. Many Americans Believe Fake news Is Sowing Confusion. Pew Research Center: Journalism & Media, 15 dez.2016. Disponível em: < <https://goo.gl/HDZh8G>>. Acesso em: 16 ago. 2018.

BBC. Russian election: biggest protests since fall of USSR. 2011. Disponível em: <http://www.bbc.com/news/world-europe-16122524>

BBC. Twitter bans RT and Sputnik ads amid election interference fears. 2017. Disponível em: <http://www.bbc.com/news/world-us-canada-41766991>

BRAUN, A. L'OTAN et la Russie: perceptions des menaces après la Géorgie. Paris: IFRI, Centre Russie/NEI, 2009.

BRYANT, Rebecca. What Kind Of Space Is Cyberspace? *Minerva* 5. P. 138-155. Londres. 2001.
DAWISHA, Karen. Putin's Kleptocracy. New York. 2016

ECKERT, D. Le Monde Russe. Paris: Hachette, 2004

FLORES, Pablo Jamilk. Inferências Falseadoras Como Base Para A Pós-Verdade. *Línguas&letras*, Cascavel (PR), v. 18, n. 41, p.20-32, 2017. Disponível em: .<<http://e-revista.unioeste.br/index.php/linguaseletras/article/view/18494/pdf>> Acesso em: 16 ago. 2018.

FOKIN, Alexander. Internet Trolling as a tool of hybrid warfare: The case of Latvia. NATO Strategic Communication Centre of Excellence. 2016.

GOVERNO FEDERAL RUSSO. Doutrina militar russa. 2010. Moscou. Disponível em: <http://carnegieendowment.org/files/2010russia_military_doctrine.pdf>. Acesso em: 16/08/2018.

HIGGINS, Kathleen. Post-truth: a guide for the perplexed. *Nature*, [s.l.], v. 540, n. 7631, p.9-9, 28 nov. 2016. Springer Nature. Disponível em:< <https://www.nature.com/news/post-truth-a-guide-for-the-perplexed-1.21054>> Acesso em: 16 ago. 2018

JATOBÁ, Daniel. Teoria das Relações Internacionais. Editora Saraiva: São Paulo, 2013.

KOVACK, Bill; ROSENSTIEL, Tom. Os elementos do jornalismo: o que os jornalistas devem saber e o público exigir. São Paulo: Geração Editorial, 2003.

LIBICKI, Martin. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press, 2007. Cambridge.

LESLIE, S. The Cold War and the American science. New York: Columbia University, 1993.

MUZAT, Numa; SERRANO, Franklin. A geopolítica das relações entre a Federação Russa e os EUA: da “cooperação” ao conflito. In: *Revista OIKOS*, v. 11, nº 1. Rio de Janeiro, 2011.

NEWMAN, Nic; FLETCHER, Richard; LEVY, David A. L.; NIELSEN, Rasmus Kleis. Digital News Report. Reuters Institute for the Study of Journalism, 2016. Disponível em: <<https://goo.gl/GxsC3R>>. Acesso em: 16 ago. 2018

NYE, Joseph S. Cyber Power. Harvard Kennedy School. Belfer Center. 2010. Disponível em: <<https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>>

MANNES, Ryan. Cyber policy as a source of power. *Russia in Cyberspace*. London. 2015.

PARKER, Emily. Putin’s Cyberphobia. 2014

RAMONET, Ignacio. A explosão do jornalismo: das mídias de massa à massa de mídias. São Paulo: Publisher Brasil, 2012.

RAMOS, Hugo. Redes Abertas, Regimes Fechados: A ilusão do poder na era digital russa. Lisboa, 2012.

REVERON, Derek S. Cyberspace and National Security: Threats, opportunities, and Power in a virtual world. Georgetown: Georgetown University Press, 2012. 272

RT. Role of Hillary Clinton in Lybia war exposed. 2016. Disponível em: <https://www.rt.com/usa/334400-hillary-clinton-libya-role/>

ROBERTS, J. M. Twentieth Century: the history of the world 1900 to 2000. New York: Penguin Group, 1999.

SANTOS JUNIOR, Roberto Lopes. Análise sobre o desenvolvimento do campo de estudo em informação científica e técnica nos Estados Unidos e na antiga União Soviética durante a Guerra Fria (1945-1991). In: Revista Brasileira de Biblioteconomia e Documentação, v. 8, n. 2, p. 130-157. São Paulo, 2012.

SARAIVA, José Flávio Sombra. História das Relações Internacionais Contemporâneas: da sociedade internacional do século XIX à era da globalização. 2º edição. São Paulo: Saraiva, 2007.

SILVERMAN, Craig. This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. BuzzFeed News. Canada, 16 nov. 2016. Disponível em: <<https://goo.gl/g6pEXb>>. Acesso em: 16 ago. 2018

STATEWATCH. Russia: Surveillance of communications. Rússia, 2000. Disponível em: <<http://database.statewatch.org/article.asp?aid=2776>> Acesso em: 11 jan. 2019

The Guardian. DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach. 2016. Disponível em: <https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2>

The Independent. Vladimir Putin hints at ‘patriotic’ private hackers interference in US election. 2017. Disponível em: <http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html>

U.S Department of Defense. The DoD Cyber Strategy. Disponível em: <
https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>

VIZENTINI, Paulo G. Fagundes. Da Guerra Fria à Crise, Porto Alegre: Editora da Universidade, 1990.

Wired. Russia's Fancy Bear hackers. Disponível em:
<https://www.wired.com/story/fancy-bear-hotel-hack/>